CLAIMS

1. A method for end-to-end data protection in a computer, comprising:

associating a data integrity field with data transferred along a data path in a computer; and

associating a virtual end-to-end address with said data integrity field, wherein said virtual end-to-end address transfers encoded information to a controller through at least one address of a read and write request thereof, wherein said encoded information identifies an offending entity within said data path.

2. The method of claim 1 wherein said controller comprises a memory controller of said computer.

3. The method of claim 1 further comprising configuring said virtual end-to-end address to further comprise at least one index and at least offset, wherein said at least one index and said at least one offset can each be varied in size to match a requirement of said controller of said computer.

4. The method of claim 1 further comprising configuring said virtual end-to-end address to further comprise at least one end-to-end bit, which is recognizable by said controller.

5. The method of claim 1 further comprising associating an end-to-end access list with said virtual end-to-end address, wherein said end-to-end access list contains at least one entry for every data transfer request provided to an interface device.

6. The method of claim 5 wherein said interface device comprises a host interface chip.

7. The method of claim 5 wherein said interface devices comprises a drive interface chip.

8. The method of claim 1 further comprising locating a buffer address within a local memory associated with said controller.

9. The method of claim 1 further comprising configuring said data integrity field to include at least one reference tag, at least one meta tag and at least one guard field, wherein said at least one meta tag comprises a static value and said at least one reference tag comprises an incrementing value.

10. A system for end-to-end data protection in a computer, said system comprising:

a data integrity field associated with data transferred along a data path in a computer; and

a virtual end-to-end address, which is associated with said data integrity field, wherein said virtual end-to-end address transfers encoded information to a controller through at least one address of a read and write request thereof, wherein said encoded information identifies an offending entity within said data path.

12. The system of claim 10 wherein said controller comprises a memory controller of said computer.

13. The system of claim 10 wherein said virtual end-to-end address comprises at least one index and at least offset, wherein said at least one index and said at least one offset can each be varied in size to match a requirement of said controller of said computer.

14. The system of claim 10 wherein said virtual end-to-end address comprises at least one end-to-end bit, which is recognizable by said controller.

15. The system of claim 1 further comprising an end-to-end access list associated with said virtual end-to-end address, wherein said end-to-end access list contains at least one entry for every data transfer request provided to an interface device.

16. The system of claim 15 wherein said interface device comprises a host interface chip.

17. The system of claim 15 wherein said interface devices comprises a drive interface chip.

18. The system of claim 10 further comprising a buffer address and a local memory associated with said controller, wherein said buffer address is located within said local memory associated with said controller.

19. The system of claim wherein said data integrity field includes at least one reference tag, at least one meta tag and at least one guard field, wherein said at least one meta tag comprises a static value and said at least one reference tag comprises an incrementing value.

20. A system for end-to-end data protection in a computer, said system comprising:

a memory controller within a computer;

a data integrity field associated with data transferred along a data path in said computer, wherein said data integrity field includes at least one reference tag, at least one meta tag and at least one guard field, wherein said at least one meta tag comprises a static value and said at least one reference tag comprises an incrementing value;

a virtual end-to-end address, which is associated with said data integrity field, such that said virtual end-to-end address comprises at least one index, at least offset and at least one end-to-end bit, which is recognizable to said memory controller, and wherein said virtual end-to-end address transfers encoded information to said memory controller through at least one address of a read and write request thereof, such that said encoded information identifies an offending entity within said data path;

an end-to-end access list associated with said virtual end-to-end address, wherein said end-to-end access list contains at least one entry for every data transfer request provided to an interface device; and

a buffer address and a local memory associated with said memory controller, wherein said buffer address is located within said local memory associated with said memory controller.